Can. J. Math., Vol. XXX, No. 5, 1978, pp. 1016–1028

FAMILIES OF GENERALIZED WEIGHING MATRICES

GERALD BERMAN

Generalized weighing (GW) matrices are orthogonal matrices whose non-zero entries are roots of unity. Several families are constructed with the aid of finite geometries which include as special cases interesting examples of conference matrices and weighing matrices. The concept of negacyclic matrices is generalized to ω-circulant matrices where $\omega \neq 1$ is a d-th root of unity and it is shown that the rows and columns of a family of GW matrices constructed from $EG(t, p^n)$ can be permuted so that the resulting matrices are ω-circulant. It is also shown that these matrices correspond to a family of relative difference sets. A second family of GW matrices is constructed from the projective geometry $PG(t, p^n)$ which are ω-circulant but which do not correspond to difference sets. The method gives a simple construction for a μ-fold spread of $(t - 2)$-spaces of $PG(t, p^n)$. Finally another family of GW matrices is constructed from $EG(t, p^n)$ in a different way. It is conjectured that these are not equivalent to ω-circulant matrices.

1. Introduction. A *generalized weighing* (GW) matrix $W(d, k, m)$ is a square $m \times m$ matrix all of whose non-zero entries are d-th roots of unity such that $AA^* = kI$ where $A^* = (\overline{a_{ij}'})$ is the conjugate transpose of A and $I = I_n$. It follows that $\sqrt{k}A$ is a unitary matrix so that $A^*A = kI$ and every row and column of A has exactly k nonzero entries.

Weighing matrices, the special case $W(2, k, m)$, have been studied extensively. The name comes from their application in accuracy of measurements by Yates [**17**]. They have recently been studied in connection with combinatorial designs by Mullin [**9**], Mullin and Stanton [**10**], and Berman [**2**; **3**]. An application ot coding theory has been considered by Pless [**12**]. Related negacyclic codes were first studied by Berlekamp [**1**]. *Hadamard matrices* are the special cases $W(2, k, k)$ in which there are no zero entries. *Generalized Hadamard matrices* $W(d, k, k)$ were considered by Butson [**4**; **5**]. These matrices have also been studied in connection with combinatorial designs by Shrikhande [**15**] and in connection with codes by Delsarte and Goethals [**6**]. The special case $W(2, m - 1, m)$ are C-matrices or conference matrices which were studied by Goethals and Seidel [**8**]. Negacyclic C-matrices were considered by Delsarte, Goethals and Seidel [**7**].

Many of the properties of weighing matrices and generalized Hadamard matrices also hold for GW matrices. Equivalent matrices are obtained by permutations of rows and columns. If a row or column of $W(d, k, m)$ is multi-

Received May 18, 1977.

https://doi.org/10.4153/CJM-1978-086-8 Published online by Cambridge University Press

plied by a d-th root of unity the resulting matrix is an equivalent $W(d, k, m)$. This implies that a normalized form can be defined in which the first entry of each row and column is 1 and if the first 1 in the j-th column (row) occurs in position λ_j, then $\lambda_j \leqq \lambda_k$ for $j \leqq k$.

New GM matrices can be constructed from known matrices just as in the case of Hadamard matrices or weighing matrices. For example, if a row or column of $W(d, k, m)$ is multiplied by an e-th root of unity the result is a $W(LCM(d, e), k, m)$. New GW matrices can also be obtained in terms of the Kronecker product: if A_1 is a $W(d_1, k_1, m_1)$ and A_2 is a $W(d_2, k_2, m_2)$ then $A_1 \times A_2$ is a $W(LCM(d_1, d_2), k_1k_2, m_1m_2)$. Such constructions may be used to obtain new GM matrices from those constructed in this paper.

In Section 2 collineations of order r in $EG(t, p^n)$ are used to construct GW matrices $W(d, p^{(t-1)n}, (p^{tn} - 1)/r)$ for every divisor of r, where r is any factor of $p^n - 1$. If p is odd, and $d = t = 2$, $r = p^n - 1$, the corresponding GW matrix $W(2, p^n, p^n + 1)$ is a conference matrix. The weighing matrices constructed in [**2**] are also a special case.

In Section 3 ω-circulant matrices are defined which generalize negacyclic matrices. It is shown that the rows and columns of the matrices constructed in Section 2 can be permuted into this form. The ideas are illustrated by constructing a number of ω-circulant matrices associated with $EG(2, 11)$ including a $W(2, 11, 12)$. It is shown in Section 4 that this family of GW matrices is in 1-1 correspondence with a family of cyclic relative difference sets which parameters $(q, s, p^{(t-1)n}, p^{(t-2)n}/r)$ where $q = (p^{tn} - 1)/(p^n - 1)$ and $rs = p^n - 1$ analogous to those constructed by Butson [**5**] for generalized Hadamard matrices.

In Section 5 it is shown that a similar construction can be carried out in $PG(t, p^n)$ to obtain another family of GW matrices $W(d, p^{(t-1)n}, q/(p^n + 1))$ where t is odd and $d|p^n + 1$, which are also ω-circulant but are not associated with relative difference sets as in the case of the family of Section 3. Instead it is shown that these matrices correspond to μ-fold spreads of $(t - 2)$-spaces of $PG(t, p^n)$. As an example the ω-circulant matrix $W(3, 15, 21)$ associated with $PG(5, 2)$ is constructed. This leads to the determination of a 5-fold spread of the 3-spaces of $PG(5, 2)$ in a different way than that given in Rao [**13**].

In Section 6 any subgroup of the additive group of $GF(p^n)$ is used to construct a GW matrix $W(p, p^{(t-1)n}, p^{tn-\alpha})$ for any α, $1 \leqq \alpha \leqq n$. The construction is a generalization of the method used by Vanstone and Mullin [**16**] to construct weighing matrices in the special case $p = 2$. It is conjectured that the rows and columns of these matrices cannot be permuted so that the resulting matrix is ω-circulant.

2. Affine *GW* matrices. The p^{tr} points of the Euclidean geometry $E = EG(t, p^n)$ can be represented by the t-tuples or column vectors

$$x = (x_1, x_2, \ldots, x_t)^T, \quad x_i \in F, i = 1, 2, \ldots, t$$

https://doi.org/10.4153/CJM-1978-086-8 Published online by Cambridge University Press

where $F = GF(p^n)$. The hyperplanes of E are the sets of points which satisfy linear equations and coefficients in F. Let P' denote the set of $p^{tn} - 1$ points not including the origin $0 = (0, 0, \ldots, 0)^T$ and let H' denote the set of $p^{tn} - 1$ hyperplanes which do not include 0. Every hyperplane $u \in H'$ satisfies a linear equation which can be expressed in the form $u_1x_1 + u_2x_2 + \ldots + u_tx_t = 1$ with not all u_i zero, so that the elements of H' can be represented by the set of t-tuples or row vectors

$$u = (u_1, u_2, \ldots, u_t), \quad u_i \in F, i = 1, 2, \ldots, t$$

with $u \neq (0, 0, \ldots, 0)$. Using matrix notation the equation satisfied by $u \in H'$ can be written as

$$(2.1) \quad ux = 1, \quad x \in P', \quad u \in H',$$

and we say that the point x is *on* the hyperplane u or u *contains* the point x and write $x \in u$ if the pair x, u satisfies (2.1). It follows that a point $x \in P'$ is on $p^{(t-1)n}$ hyperplanes of H' and a hyperplane $u \in H'$ contains $p^{(t-1)n}$ points of P'.

A *collineation* ϕ is a transformation of E which preserves collinearity. The *order* of ϕ is the smallest integer r such that ϕ^r is the identity transformation. Let ϕ_λ denote the mapping defined by

$$(2.2) \quad \phi_\lambda x = \lambda x = (\lambda x_1, \lambda x_2, \ldots, \lambda x_t)$$

where λ is a nonezro element of F.

LEMMA 2.1. *The mapping ϕ_λ, $\lambda \in F$, $\lambda \neq 0$ is a collineation of E which maps the hyperplane u onto the hyperplane $\lambda^{-1}u$, i.e.,*

$$(2.3) \quad \phi_\lambda u = \lambda^{-1}u = (\lambda^{-1}u_1, \lambda^{-1}u_2, \ldots, \lambda^{-1}u_t).$$

If $\lambda \neq 1$ there are no fixed points in P' or fixed hyperplanes in H' under the mapping ϕ_λ. The order r_λ of ϕ_λ is a factor of $p^n - 1$, and if $r|p^n - 1$ there is a λ such that $r_\lambda = r$.

The points x, y, z of P' are collinear if there exists elements $a, b, c \in F$ not all zero such that $ax + by + cz = 0$, $a + b + c = 0$. It follows that

$$a(\phi_\lambda x) + b(\phi_\lambda y) + c(\phi_\lambda z) = \lambda(ax + by + cz) = 0$$

so that ϕ_λ is a collineation. For every $x \in u$, $(\lambda^{-1}x)(\lambda u) = 1$ so that $\lambda^{-1}u$ contains $\phi_\lambda x$, that is $\phi_\lambda u = \lambda^{-1}u$. The mapping ϕ_λ has no fixed points or hyperplanes since very point $x \in P'$ and every $u \in H'$ has at least one nonzero component implying that $\phi_\lambda x \neq x$, $\phi_\lambda u \neq u$ provided $\lambda \neq 1$. Finally $\phi_\lambda{}^k x = \lambda^k x$ so that the order of ϕ_λ is the same as the multiplicative order of λ in F, which divides $p^n - 1$. Further if $r|p^n - 1$ there are elements of F of order r. For these elements $r_\lambda = r$.

Let ϕ_λ have order r_λ and set

$$[x] = \{\phi_\lambda{}^k x, k = 0, 1, \ldots, r_\lambda - 1\}, \quad x \in P'.$$

https://doi.org/10.4153/CJM-1978-086-8 Published online by Cambridge University Press

It is immediate that $y \in [x]$ if and only if $x \in [y]$ so that we can choose elements $x^1, x^2, \ldots, x^m \in P'$, $r_\lambda m = p^{tm} - 1$ such that $[x^1] \cup [x^2] \cup \ldots \cup [x^m]$ is a partition of P'. Similarly if we set

$$[u] = \{\phi_\lambda{}^k u,\ k = 0, 1, \ldots, r_\lambda - 1\}, \quad u \in H'$$

there exist elements $u^1, u^2, \ldots, u^m$ such that $[u^1] \cup [u^2] \cup \ldots \cup [u^m]$ is a partition of H'. Since the hyperplanes $\phi_\lambda{}^k u^i$ are parallel the point x^j lies on at most one of them. If x^j is a point of $\phi_\lambda{}^l u^i$, i.e., $(\phi_\lambda{}^l u^i)x^j = 1$, then $(\lambda^{-k}(\phi_\lambda{}^l u^i))(\lambda^k x^j) = 1$ so that $\phi_\lambda{}^k x^j$ is a point of $\phi_\lambda{}^{l+k} u^i$, $k = 0, 1, \ldots, r_\lambda - 1$. If points of $[x^j]$ are on hyperplanes of $[u^i]$ we shall write $[x^j] \in [u^i]$ for convenience. It follows from the above remarks that if $[x^j] \in (u^i]$ there exists a unique integer $h = \nu(u^i, x^j)$ say, such that $\phi_\lambda{}^h x^j$ is a point of u^i; otherwise x^j is not a point of any of the hyperplanes of $[u^i]$.

Let $d > 1$ denote any divisor of r_λ and let $\omega \neq 1$ be a d-th root of unity. Let $A(\phi_\lambda, x^1, x^2, \ldots, x^m, u^1, u^2, \ldots, u^m, \omega)$ denote the $m \times m$ matrix (a_{ij}) defined by

$$(2.4) \quad a_{ij} = \begin{cases} \omega^{\nu(u^i, x^j)} & \text{if } [x^i] \in [u^j] \\ 0 & \text{otherwise} \end{cases}$$

for $i, j = 1, 2, \ldots, m$ where $r_\lambda m = p^{tn} - 1$.

THEOREM 2.2. *Let ϕ_λ denote a collineation of order r_λ of $EG(t, p^n)$ as defined by 2.2 (and (2.3)). Let $d|r_\lambda$ and let $\omega \neq 1$ be a d-th root of unity. Then the matrix $A = A(\phi_\lambda, x^1, x^2, \ldots, x^m, u^1, u^2, \ldots, u^m)$ is a GW matrix $W(d, p^{(t-1)n}, (p^{tn} - 1)/r_\lambda)$.*

From the construction A is an $m \times m$ matrix, $r_\lambda m = p^{tn} - 1$, whose nonzero elements are d-th roots of unity. Since there are $p^{(t-1)n}$ points on every hyperplane and every set $[x^j]$ can contain at most one of these points, every row of A contains exactly $p^{(t-1)n}$ nonzero entries.

It remains to be shown that A is orthogonal, i.e., that the sum

$$(2.5) \quad Q = \sum_j a_{ij}\bar{a}_{kj}$$

equals 0 for $i \neq k$. If u^i, u^k are parallel, then none of the hyperplanes of $[u^i]$ have points in common with hyperplanes of $[u^k]$ so that $Q = 0$. If u^i, u^k intersect there are nonzero terms in the sum Q corresponding to every point x^j which is common to a hyperplane of $[u^i]$ and a hyperplane of $[u^k]$. From the previous discussion the hyperplane u^i intersects each of the hyperplanes $\phi_\lambda{}^h u^k$, $h = 0, 1, \ldots, r_\lambda - 1$ in $p^{(t-1)n}$ points so that the sum (2.5) contains $r_\lambda p^{(t-2)n}$ nonzero terms. For any point $\phi_\lambda{}^l x^j$ on u^i and $\phi_\lambda{}^h u^j$ we have

$$u^i(\phi_\lambda{}^l x^j) = 1, \quad (\phi_\lambda{}^h u^k)(\phi_\lambda{}^l x^j) = u^k(\phi_\lambda{}^{l-h} x^j) = 1$$

so that $\nu(u^i, x^j) = l$, $\nu(u^k, x^j) = l - h$ and by (2.4) $a_{ij} = \omega^l$, $a_{kj} = \omega^{l-h}$, $a_{ij}\bar{a}_{kj} = \omega^h$. This means that for every $h = 0, 1, \ldots, r_\lambda - 1$ there are $p^{(t-2)n}$

https://doi.org/10.4153/CJM-1978-086-8 Published online by Cambridge University Press

terms of Q which have value ω^h and we have

$$Q = p^{(t-2)n}(1 + \omega + \omega^2 + \ldots + \omega^{r_\lambda - 1}) = 0$$

since ω is a d-th root of unity and $d|r_\lambda$.

COROLLARY 2.3. *Let p, t, r, d denote any positive integers such that p is prime, $d|r$ and $r|p^n - 1$. Then there exists a GW matrix $W(d, p^{(t-1)n}, (p^{tn} - 1)/r)$.*

By Lemma 2.1 there exists a λ such that the collineation ϕ_λ is of order r for any r which is a factor of $p^n - 1$. The required matrix is given by Theorem 2.2.

3. ω-circulant matrices. Let $\omega \neq 1$ denote a d-th root of unity. A GW matrix A is *ω-circulant* if the i-th row of A is

$$(3.1) \quad \omega a_{n-i+2}, \omega a_{n-i+3}, \ldots, \omega a_n, a_1, a_2, \ldots, a_{n-i+1}$$

where $a_1, a_2, \ldots, a_n$ is the first row of A. In the special case $d = 2$, A is a *negacyclic matrix* as defined in [**7**]. In this section it will be shown that the rows and columns of any GW matrix $W(d, k, m)$ constructed in Section 2 can be permuted so that the resulting matrix is an ω-circulant matrix.

Let K denote $GF(p^{tn})$ considered as an extension field of $F = GF(p^n)$ and let x denote a primitive element of K. The points of P' (the points of $EG(t, p^n)$ $\neq 0$) can be represented by the powers $x, x^2, \ldots, x^{v'} = 1$, $v' = p^{tn} - 1$. It is easy to verify that the mapping χ' defined by $\chi' x^j = x^{j+1}$ is a collineation. Rao [**13**] showed that χ' is also transitive on the hyperplanes of H' (the hyperplanes of $EG(t, p^n)$ which do not contain 0).

Let $q = (p^{tn} - 1)/(p^n - 1)$; then the nonzero elements of F have the unique representation x^{jq}, $j = 0, 1, \ldots, p^n - 2$. Let r be a factor of $p^n - 1$, $rs = p^n - 1$; then $x^{sq} \in F$ and the mapping $\psi_r = (\chi')^{sq}$ is a collineation of order r and is a mapping ϕ_λ of Section 2 with $\lambda = x^{sq}$. Set $m = sq$ and let $x^j = \chi^j x$, $j = 1, 2, \ldots, m$. If u is any hyperplane of H' set $u^i = \chi^i u = \{x^{j+i}, x^j \in u\}$, $i = 1, 2, \ldots, m$. (Note that the superscript in x^j is also a power of x in this case).

THEOREM 3.1. *Let $r|p^n - 1$, $rs = p^n - 1$, $m = sq$, and let $\psi_r, x^1, x^2, \ldots, x^m$, $u^1, u^2, \ldots, u^m$ be defined as above. Let $d|r$, $\omega \neq 1$ be a d-th root of unity, and let $B = (b_{ij}) = (\mathrm{A}\psi_s, x^1, x^2, \ldots, x^m, u^1, u^2, \ldots, u^m)$ as defined in Section 2. Then B is a ω-circulant GW matrix $W(d, p^{(t-1)n}, m)$.*

Let $\psi_r{}^h x^j$ be a point of u^i so that $\nu(u^i, x^j) = h$ and $b_{ij} = \omega^h$. Then $\chi' \psi_r{}^k x^j$ is a point of $\chi' u^i$. If $j < m$, $\chi' \psi_r{}^h x^j = \psi_r{}^h \chi' x^j = \psi_r{}^h x^{j+1}$ so that $b_{i+1, j+1} = \omega^h$. If $j = m$ then $\psi_r{}^h x^{j+1} = \psi_s{}^{h+1} x$ is in u^{i+1} and $b_{i+1,1} = \omega^{h+1}$. This implies 3.1 so that B is ω-circulant.

Several corollaries are immediate.

COROLLARY 3.2. *If p, t, r and d are positive integers such that p is prime, $d|r$ and $r|p^n - 1$ there exists an ω-circulant matrix $W(d, p^{(t-1)n}, (p^{tn} - 1)/r)$.*

https://doi.org/10.4153/CJM-1978-086-8 Published online by Cambridge University Press

COROLLARY 3.3. *If p is an odd prime there exists a negacyclic matrix $W(2, p^{(t-1)n}. (p^{tn} - 1)/r)$ for every even factor r of $p^n - 1$.*

COROLLARY 3.4. *There exists an ω-circulant conference matrix $W(d, p^n, p^n + 1)$ for every divisor d of $p^n - 1$.*

The first corollary is a restatement of the theorem. The second corollary is obtained by taking $d = 2$ where $r = 2r'$ and the third corollary by taking $r = p^n - 1$. If p is odd the matrix in Corollary 3.4 becomes a negacyclic conference matrix if we take $d = 2$ (which is a divisor of $p^n - 1$).

The above ideas are illustrated in the following example. Consider $EG(2, 11)$. The polynomial $x^2 = 10x + 4$ is a primitive polynomial so that the 120 points $\neq 0$ can be represented by the powers $x, x^2, \ldots, x^{120} = 1$. Using the tables given in Rao [**13**] it is easy to verify that the points in the hyperplane $u = (0, 1) \in H'$ are given by

$$(3.2) \quad u = \{1, 6, 22, 62, 68, 69, 71, 88, 99, 103, 113\}$$

recording only the powers of x. Since the divisors $\neq 1$ of $p^n - 1 = 10$ are 10, 5, 2 the collineations which determine GW matrices are $\psi_{10} = \chi'^{12}$, $\psi_5 = \chi'^{24}$ and $\psi_2 = \chi'^{60}$.

The collineation ψ_{10} determines three generalized conference matrices. If we write the points of u in terms of ψ_{10} we have

$$u = \{1, \psi_{10}{}^5 2, \psi_{10}{}^8 3, \psi_{10}{}^6 4, \psi_{10}{}^9 5, 6, \psi_{10}{}^8 7, \psi_{10}{}^5 8, \psi_{10}{}^5 9, \psi_{10} 10, \psi_{10}{}^5 11\}$$

and if we let $\omega_{10} \neq 1$ be a 10-th root of unity the first row of the corresponding ω_{10}-circulant generalized conference matrix $W(10, 11, 12)$ is

$$0, 1, \omega_{10}{}^5, \omega_{10}{}^8, \omega_{10}{}^6, \omega_{10}{}^9, 1, \omega_{10}{}^8, \omega_{10}{}^5, \omega_{10}{}^5, \omega_{10}, \omega_{10}{}^5.$$

If $\omega_5 \neq 1$ is a 5-th root of unity, the first row of the ω_5-circulant generalized conference matrix $W(5, 11, 12)$ is

$$0, 1, 1, \omega_5{}^3, \omega_5, \omega_5{}^4, 1, \omega_5{}^3, 1, 1, \omega_5, 1$$

and if we take $\omega = -1$ we obtain the conference matrix with first row

$$0, 1, -1, 1, 1, -1, 1, 1, -1, -1, -1, -1.$$

In terms of the collineation ψ_5 (3.2) can be rewritten as

$$u = \{1, \psi_5{}^4 3, 6, \psi_5{}^4 7, \psi_5{}^2 14, \psi_5{}^3 16, \psi_5{}^4 17, \psi_5{}^2 20, \psi_5{}^2 21, 22, \psi_5{}^2 23\}.$$

Let $\omega_5 \neq 1$ be a 5-th root of unity as before. Then the first row of a second ω_5-circulant matrix, this time a $W(5, 11, 24)$, has first row

$$0, 1, 0, \omega_5{}^4, 0, 0, 1, \omega_5{}^4, 0, 0, 0, 0, 0, 0, \omega_5{}^2, 0, \omega_5{}^3, \omega_5{}^4, 0, 0, \omega_5{}^2, \omega_5{}^2, 1, \omega_5{}^2.$$

Similarly, using ψ_2, (3.1) becomes

$$u = \{1, \psi_2 2, 6, \psi_2 9, \psi_2 11, 22, \psi_2 28, \psi_2 29, \psi_2 39, \psi_2 43, \psi_2 53\}$$

which leads to a weighing matrix $W(2, 12, 60)$.

https://doi.org/10.4153/CJM-1978-086-8 Published online by Cambridge University Press

4. Cyclic relative difference sets. A *cyclic relative difference* (*CRD*) set $R(q, \nu, k, \lambda)$ is a subset of k integers $D = \{d_1, d_2, \ldots, d_k\}$ modulo $q\nu$ such that $d_i - d_j \neq 0 \bmod q$ for any $d_i, d_j, i \neq j$, and for every $d \neq 0 \bmod q$ there are exactly λ pairs d_i, d_j for which $d_i - d_j = d \bmod q\nu$. A *CRD* set is a special case of a difference set of a group G of order $q\nu$ relative to a normal subgroup H of order ν in which G is cyclic. If $\nu = 1$, R is an ordinary *cyclic difference set* with parameters q, k, λ. The parameters of D satisfying the identity $k(k - 1).$ $= \lambda(q - 1\nu.$

The following lemma is required.

LEMMA 4.1. *Let r be a factor of ν, $rs = \nu$ and let d_i' denote the integer d_i reduced modulo qs, $i = 1, 2, \ldots, k$ where $D = \{d_1, d_2, \ldots, d_k\}$ is an $R(q, \nu, k, \lambda)$. Then $D' = \{d_1', d_2', \ldots, d_k'\}$ is an $R(q, s, k, \lambda r)$.*

Each of the integers $d + hqs$, $h = 0, 1, \ldots, r - 1$ occurs λ times among the differences $d_i - d_j$. Each of these integers equals d modulo qs, so that d occurs $r\lambda$ times among the integers $d_i' - d_j'$ taken modulo qs.

A *CRD* set can be associated with every ω-circulant matrix constructed in Section 3.

THEOREM 4.2. *Let $B = (b_{ij})$ be the ω-circulant matrix $W(d, p^{(t-1)n}, sq)$, where $d|r$ $rs = p^n - 1$, $qrs = p^{tn} - 1$, constructed in Section 3, and let*

$$D_i = \{j|b_{ij} \neq 0\} \bmod qs, \quad i = 1, 2, \ldots, qs$$

Then D_i is a CRD set $R(q, s, p^{(t-1)n}, p^{(t-2)n}r)$ $i = 1, 2, \ldots, qs$.

Consider the set of integers

$$S_h = \{j|x^j \in u^h\} \quad \bmod q(p^n - 1).$$

We shall show that this set is a *CRD* set $R(q, p^n - 1, p^{(t-1)n}, p^{(t-2)n})$. First note that S_i contains $p^{(\ -1)n}$ integers so that $k = p^{(t-1)n}$. Suppose $i - j = d$ and $x^i, x^j \in u^h$. Then $\chi'^d x^j = x^i$ so that $x^i \in \chi'^d u^h = u^{h+d}$. It follows that $d_i - d_j$ has a solution in S_h whenever x^i is on the hyperplanes u^h, u^{h+d}. Since these hyperplanes are not parallel they have $p^{(t-2)n}$ points in common and $\lambda = p^{(t-2)n}$. No difference can be a multiple of q. For if $i - j = kq$ the points $x^i = x^{j+kq} = \alpha x^j$ and x^j are in u^h, where $\alpha \in F$. It follows that u^i contains the origin and so could not be in H', a contradiction. The hyperplanes u^h and u^{h+lq} are parallel for every l.

Now consider D_i. If $r = 1$, i.e., if $s = p^n - 1$ the above remarks show that the theorem holds. If $r \neq 1$, then $D_\imath$ can be obtained from S_i by reducing the integers of S_i modulo qs. To see this note that the ith row of B corresponds to the set $[u^i]$. If $b_{ij} = \omega^h$ then u^i contains the point x^{j+hsq}. That is, if x^l is a point of u^i, $l = j + hsq$ so that $l \in S_i$, $b_{ij} \neq 0$ and $j \in D_i$. The result now follows from Lemma 4.1 since $j \equiv l \bmod sq$.

https://doi.org/10.4153/CJM-1978-086-8 Published online by Cambridge University Press

COROLLARY 4.3. *Let p, t, n be positive integers such that p is prime and $t > 1$. Then there exists an ordinary cyclic difference set with parameters* $((p^{tn} - 1)/(p^n - 1), p^{(t-1)n}, p^{(t-2)n}(p^n - 1))$.

This follows from the theorem by taking $r = p^n - 1$, $s = 1$.

5. Projective ω-circulant matrices. In this section a cyclic collineation in $PG(t, p^n)$ is used to construct ω-circulant matrices which do not correspond to relative difference sets as in the case of affine ω-circulant matrices of Section 3.

The set of q_t points of $PG(t, p^n)$, where $q_j = (p^{(j+1)n} - 1)/(p^n - 1)$, can be represented by the powers $x, x^2, \ldots, x^{q_t} = 1$ of a primitive element of $K = GF(p^{(t+1)n})$. The points of a σ-flat are the points linearly dependent on $\sigma + 1$ linearly independent elements with respect to the subfield $F = GF(p^n)$, $\sigma = 0, 1, \ldots, t - 1$. A point is a 0-flat and a hyperplane is a $(t - 1)$-flat. A collineation of $PG(t, p^n)$ is a transformation of the set of points P which maps σ-spaces on σ-spaces for all $\sigma = 1, 2, \ldots, t - 1$. Singer [**14**] showed that the mapping χ defined by $\chi x^j = x^{j+1}$ is a collineation which is transitive on the set H of hyperplanes as well as transitive on the set P, i.e., if u is any hyperplane, the hyperplanes $\chi^i u$, $i = 1, 2, \ldots, q_t$ are distinct and thus represent all elements of H.

A μ-fold spread Σ of σ-spaces is a collection of σ-spaces such that each point of P occurs in exactly μ σ-spaces of Σ. Rao [**13**] proved that if $t + 1$ and $\sigma + 1$ have $\rho + 1$ as a common factor, then a μ-fold spread of σ-flats in $PG(t, p^n)$ exists, where $\mu = q_\sigma/q_\rho$. It is also shown that the σ-flats of Σ have period $\nu = q_t/q_\rho$, (under the collineation χ) and if S is a σ-space of Σ, then all the σ-spaces of Σ can be represented in the form $S, \chi S, \ldots, \chi^{\nu-1}S$.

LEMMA 5.1. *If t is odd, every $(t - 1)$ space of $PG(t, p^n)$ contains a $(t - 2)$-space which is invariant under the collineation χ^ν, where $\nu = q_t/q_1$.*

Since t is odd $\sigma = t - 2$ is odd so that $t + 1$ and $\sigma + 1$ have a factor $\rho + 1$ where $\rho = 1$. It follows from Rao's theorem that there is a μ-fold spread Σ of $(t - 2)$-spaces of period $\nu = q_t/q_1$ where $\mu = q_{t-2}/q_1$. Let S be a member of Σ. Suppose it lies in the hyperplane u; then the hyperplane $u^i = \chi^i u$ contains the σ-spaces $S_i = \chi^i S \in \Sigma$. It follows that every hyperplane contains a member of Σ. Further $\chi^\nu S_i = \chi^\nu(\chi^i S) = \chi^i(\chi^\nu S) = \chi^i S = S_i$ since ν is the period of S, showing that $S_i \in u^i$ is invariant under χ^ν.

Let t be odd and r a factor of $q_1 = p^n + 1$, say $q_1 = rs$. Then $q_t = q_1\nu = r(s\nu)$. Let $\theta_r = \chi^{s\nu}$ so that θ_r is a collineation of period r which leaves the $(t - 2)$-spaces of Σ fixed. Let

$$[x^j] = \{x^j, \theta_r x^j, \theta_r^2 x^j, \ldots\} \quad j = 0, 1, \ldots, q_t - 1.$$

The set $[x^j]$ contains r distinct elements for every j and the sets $[x], [x^2], \ldots, [x^{s\nu}]$ are disjoint and determine a partition of P. Similarly for every $u \in H$ set

$$[u] = \{u, \theta_r u, \theta_r^2 u, \ldots\}.$$

The set $[u]$ contains r elements and if we set $u^i = \chi^i u$, $i = 1, 2, \ldots, s\nu$, then the sets $[u^1], [u^2], \ldots, [u^{s\nu}]$ are disjoint and determine a partition of H.

These sets have properties similar to the corresponding sets defined in Section 2. If x^j is a point of $\theta_r^h u^i$ then $\theta_r^k x^j$ is a point of $\theta_r^{k+h} u^i$. However the hyperplanes of $[u^i]$ are not parallel. Instead they have the property that if x^j is on more than one hyperplane of $[u^i]$ it is on every hyperplane. This follows immediately from Lemma 5.1 since every pair of hyperplanes of $[u^i]$ intersect in a unique $(t - 2)$-space which must be the $(t - 2)$-space of Σ invariant under χ^ν.

We now define a matrix $C(\theta_r, \omega) = (c_{ij})$ as follows. Let $d > 1$ be a factor of r and $\omega \neq 1$ a d-th root of unity. Set

$$(5.1)\quad c_{ij} = \begin{cases} \omega^h & \text{if } \theta_r^h x^j \in T_i \\ 0 & \text{otherwise} \end{cases}$$

where T_i is the set of points of u^i not in S_i, the invariant $(t - 2)$-space of Σ.

THEOREM 5.2. *Let $r > 1$ be a factor of $q_1 = p^n + 1$, $q_1 = rs$ say, and let $d \neq 1$ be a factor of r and ω a d-th root of unity. Let $C = C(\theta_r, \omega)$ denote a matrix constructed as above. Then C is an ω-circulant matrix $W(d, p^{(t-1)n}, q_t/r)$.*

The number of points of T_i is $q_{t-1} - q_{t-2} = p^{(t-1)n}$ so that the number of nonzero elements in each row is $p^{(t-1)n}$. Also $m = s\nu = sq_t/q_1 = q_t/r$. To show that C is orthogonal, consider rows i and k and let $Q = \Sigma_j c_{ij}\overline{c_{kj}}$ analogous to (2.5). If $[u^i]$, $[u^k]$ intersect in a $(t - 2)$-space of Σ then every term of Q is zero. Otherwise a term will be equal to ω^h only if $c_{ij} = \omega^{l+h}$, $c_{kj} = \omega^l$ for some l. This implies that the hyperplanes $\theta_r^h u^i$ and u^k contain a common point $\theta_r^l x^j$ (for some j) which is not a point of S_i or S_k (the subspaces of Σ). The hyperplanes $\theta_r^h u_i$ and u^j contain q_{t-2} common points (i.e., a $(t - 2)$-space). The spaces S_i, S_k are $(t - 2)$-spaces which each intersect this common space in $(t - 3)$-spaces having a $(t - 4)$-space in common and hence determine $2q_{t-3} - q_{t-4}$ distinct points which correspond to zero terms of Q. Thus the number of common points of $\theta_r^h u^i$ and u^j which correspond to terms ω^h in Q is $q_{t-2} - 2q_{t-3} + q_{t-4}$. Since this is true for each $h = 0, 1, \ldots, r - 1$, the sum Q is equal to

$$(q_{t-2} - 2q_{t-3} + q_{t-4})(1 + \omega + \ldots + \omega^{r-1}).$$

This is zero since $\omega \neq 1$ is a d-th root of unity and $d|r$.

COROLLARY 5.3. *If p, t, n, d and r are positive integers greater than one such that p is prime, $d|r$, $r|p^n + 1$, then there exists an ω-circulant matrix $W(d, p^{(t-1)n}, (p^{(t+1)n} - 1)/r(p^n - 1))$.*

COROLLARY 5.4. *There exists an ω-circulant generalized conference matrix $W(d, p^{2n}, p^{2n} + 1)$ for every divisor d of $p^n + 1$.*

Corollary 5.3 is a restatement of the theorem and Corollary 5.4 is the special case $t = 3$, $r = p^n + 1$. If p is odd, the special case $d = 2$ is a negacyclic conference matrix.

To illustrate the above ideas consider $PG(3, 3)$. Using the primitive polynomial $x^4 = 2x^3 + 1$ and the tables in Rao [**13**] we find that the hyperplane $u = (0, 0, 0, 1)$ contains the points

(5.2) $u = \{1, 2, 3, 9, 17, 19, 24, 26, 29, 30, 35, 38, 39\}$

recording only powers of x. In this case $p^n + 1 = 4$. Taking $r = 2$, $\theta_2 = \chi^{20}$, u can be rewritten as

(5.3) $u = \{1, 2, 3, \theta_2 4, \theta_2 6, (9, \theta_2 9), \theta_2 10, \theta_2 15, 17, \theta_2 18, (19, \theta_2 19)\}$

from which we deduce the negacyclic matrix $W(2, 19, 20)$ whose first row is given by

$$0, 1, 1, 1, -1, 0, -1, 0, 0, 0, -1, 0, 0, 0, 0, -1, 0, 1, -1, 0.$$

Taking $r = 4$ $\theta_4 = \chi^{10}$, (5.2) can be rewritten as

(5.4) $u = \{\theta_4^3 0, 1, 2, 3, \theta_4^2 4, \theta_4^3 5, \theta_4^2 6, \theta_4 7, \theta_4^3 8, (9, \theta_4 9, \theta_4^2 9, \theta_4^3 9)\}$

corresponding to the ω_4-circulant generalized conference matrix $W(4, 9, 10)$ with first row

$$\omega_4^3, 1, 1, 1, \omega_4^2, \omega_4^3, \omega_4^2, \omega_4, \omega_4^3, 0$$

or if we prefer

$$0, \omega_4^3, 1, 1, 1, \omega_4^2, \omega_4^3, \omega_4^2, \omega_4, \omega_4^3$$

where $\omega_4 \neq 1$ is a 4-th root of unity. Taking $d = 2$ we have as a special case the negacyclic matrix with first row

$$0, -1, 1, 1, 1, 1, -1, 1, -1, -1.$$

In this caes Σ is a spread of lines with $\mu = 1$ $\nu = 10$. The invariant line l in u given by (5.2) is immediate from (5.4) (or 5.3), $l = \{9, 19, 29, 39\} = \{9, \theta_4 9, \theta_4^2 9, \theta_4^3 9\}$ and Σ is the set of lines $l_j = \chi^j l$, $j = 0, 1, \ldots, 9$.

This method provides a simple alternative method for obtaining Σ in case $\sigma = t - 2$. To illustrate the case $\mu \neq 1$ we find the 5 fold spread of 3-spaces of $PG(5, 2)$.

Again using the tables in Rao and using the hyperplane $u = (1, 0, 1, 0, 0, 0)$ we find the points of u are given by

(5.5) $u = \{0, 1, 2, 4, 9, 10, 12, 14, 15, 16, 19, 20, 21, 22, 24, 25, 26, 27, 28, 35, 37, 39, 42, 43, 46, 50, 53, 55, 56, 58, 59\}$

where this time the integers are taken modulo 63 and $r = 3$, $\theta_3 = \chi^{21}$, $\mu = 5$, $\nu = 21$. In term of θ_3, (5.5) has the representation

(5.6) $u = \{(0, \theta_3 0, \theta_3^2 0), (1, \theta_3^1, \theta_3^2, 1), 2, \theta_3 3, (4, \theta_3 4, \theta_3^2 4), \theta_3 5, \theta_3 6, \theta_3 7, \theta_3^2 8, 9, 10, \theta_3^2 11, 12, \theta_3^2 13, (14, \theta_3 14, \theta_3^2 14), 15, (16, \theta_3 16, \theta_3^2 16), 17, \theta_3 18, 19, 20\}$

https://doi.org/10.4153/CJM-1978-086-8 Published online by Cambridge University Press

The 3-spaces of Σ are immediate. If we set $M = \{0, 1, 4, 14, 16\}$, $\Pi = M \cup \theta_3 M \cup \theta_3{}^2 M$, the 3-spaces of Σ are given by $\Pi_i = \chi^j \Pi$, $j = 0, 1, \ldots, 20$.

The representation (5.6) also provides us with the first row of the corresponding ω_3-circulant matrix $W(3, 16, 21)$, namely

$$0, 0, 1, \omega, 0, \omega, \omega, \omega, \omega^2, 1, 1, \omega^2, 1, \omega^2, 0, 1, 0, 1, \omega, 1, 1.$$

6. Non-circulant affine *GW* matrices. A collineation in $EG(t, p^n)$ was used in Section 2 to construct a family of GW matrices which were shown to be ω-circulant in Section 3. In this section a different method is used to construct another family of GW matrices related to $EG(t, p^n)$.

Let the p^{tn} points of $EG(t, p^n)$ be represented as pairs (x, y) where $x = (x_1, x_2, \ldots, x_{t-1})^T$, $x_1, x_2, \ldots, x_{t-1}, y \in F = GF(p^n)$. Let the pairs (u, v), $u = (u_1, u_2, \ldots, u_{t-1})$, $u_1, u_2, \ldots, u_{t-1}, v \in F$ represent the hyperplanes

$$(6.1) \quad y = ux + v$$

i.e., the point $z = (x, y)$ is on the hyperplane $w = (u, v)$ if (6.1) is satisfied. Let G denote any subgroup of order p^α $(1 \leqq \alpha \leqq n)$ of the additive group F^+ of F. If z is in the hyperplane w then $z + g = (x, y + g)$ is on the hyperplane $w + g = (u, v + g)$ for all $g \in G$. Further the hyperplanes $w + g$ are parallel for all $g \in G$.

Let P'' denote the set of points z of $EG(t, p^n)$ and H'' the set of hyperplanes w satisfying (6.1). Let

$$[z] = \{z + g, g \in G\}, \quad [w] = \{w + g, g \in G\}.$$

This mapping $z \rightarrow [z]$ clearly determines a partition of P'' and the mapping $w \rightarrow [w]$ a partition of H''. Let $z^1, z^2, \ldots, z^\beta$, $\beta = p^{tn-\alpha}$ denote any set of points such that the sets $[z^1], [z^2], \ldots, [z^\beta]$ are disjoint and determine a partition of P'' and similarly let $w^1, w^2, \ldots, w^\beta$ denote hyperplanes such that $[w^1], [w^2], \ldots, [w^\beta]$ is a partition of H''.

If a point z is on a hyperplane $w + g$ then $z + g'$ is on the hyperplane $w + g + g'$. Since the hyperplanes $w + g$, $w + g + g'$ are parallel the point $z + g'$ cannot lie on the hyperplane w. Thus only one point of $[z]$ can be on any hyperplane of $[w]$, and if z lies on a hyperplane of $[u]$ as also does $z + g$ for every $g \in G$.

The elements of G can be represented as $g = (g_1, g_2, \ldots, g_\alpha)$ where g_j, $j = 1, 2, \ldots, \alpha$ are residue classes of integers modulo p. Let $\gamma(g) = g_1 + g_2 + \ldots + g_\alpha \bmod p$ and let $\omega \neq 1$ denote a p-th root of unity. Let $D(G)$ denote the $\beta \times \beta$ matrix (d_{ij}) defined by

$$(6.2) \quad d_{ij} = \begin{cases} \omega^{\alpha(g)} & \text{if } z^j \in w^i + g \\ 0 & \text{otherwise} \end{cases}$$

for $i, j = 1, 2, \ldots, \beta$.

https://doi.org/10.4153/CJM-1978-086-8 Published online by Cambridge University Press

THEOREM 6.1. *Let G denote a subgroup of F^+ or order p^α $(1 \leqq \alpha \leqq n)$ and let $D(G)$ be a $\beta \times \beta$ matrix constructed as above. Then $D(G)$ is a GW matrix $W(p, p^{(t-1)n}, \beta)$.*

From the above remarks the number of nonzero entries in any row equals the number $p^{(t-1)n}$ of points on a hyperplane of $EG(t, p^n)$. To prove $D(G)$ is orthogonal consider the i-th and k-th rows and the sum $Q = \bigcup_j d_{ij}\overline{d_{kj}}$ where d_{ij}, d_{kj} are defined by (6.2). Each term is 0 or ω^h for $0 \leqq h \leqq p - 1$. Suppose $g \in G$ and $\gamma(g) = h$. If $w^i + g$ and w^k intersect in a point $z^j + g'$ with $\gamma(g') = h'$, then $z^j \in w^i + g - g'$, $z^j \in w^k - g$, $\gamma(g - g') = h - h'$ and $\gamma(-g') = -h'$ so that $d_{ij} = \omega^{h-h'}$, $d_{kj} = \omega^{-h'}$, $d_{ij}\overline{d_{kj}} = \omega^h$. Since the hyperplanes $w^i + g$, w^k intersect in $p^{(t-2)n}$ points there are $p^{(t-1)n}$ terms of Q equal to ω^h corresponding to g. But there are p^{n-1} elements of $g \in G$ such that $\gamma(g) = h$ so that there are $p^{n-1}p^{(t-2)n} = p^{(t-1)n-1}$terms of Q equal to ω^h. Since this number is the same for all $h = 0, 1, \ldots, p - 1$,

$$Q = p^{(t-1)n-1}(1 + \omega + \ldots + \omega^{h-1}) = 0.$$

COROLLARY 6.2. *If p, t, n and α are positive integers such that p is prime $t > 1$ and $1 \leqq \alpha \leqq n$, then there exists a GW matrix $W(p, p^{(t-1)n}, p^{tn-\alpha})$.*

Notice that if G_α denotes a subgroup of order p^α then there is a nest of subgroups

$$G_1 \subset G_2 \subset \ldots \subset G_n = F^+.$$

It follows that the corresponding matrices $D(G_1)$, $D(G_2)$, $\ldots$, $D(G_n)$ can be constructed sequentially. Each element of $D(G_j)$ corresponds in an abvious way to a $p \times p$ submatrix of $D(G_{j-1})$, $j = 2, \ldots, n$.

It is conjectured that the GW matrices $D(G)$ constructed in this way are not equivalent to ω-circulant matrices.

REFERENCES

1. E. R. Berlekamp, *Algebraic coding theory* (McGraw Hill, New York, 1968).
2. Gerald Berman, *Weighing matrices and group divisible designs determined by $EG(t, p^n)$, $t > 2$*, Utilitas Mathematica *12* (1977), 183–191.
3. ——— *Familites of skew circulant weighing matrices*, Ars Combinatoria *4* (1977), 293–307.
4. A. T. Butson, *Generalized Hadamard matrices*, Proc. Amer. Math. Soc. *13* (1962), 894–898.
5. ——— *Relations among generalized Hadamard matrices, relative difference sets and maximal length recurring sequences*, Can. J. Math. *15* (1963), 42–48.
6. P. Delsarte and J. M. Goethals, *Tri-weight codes and generalized Hadamard matrices*, Information and Control *15* (1969), 192–206.
7. P. Delsarte, J. M. Goethals and J. J. Seidel, *Orthogonal matrices with zero diagonal, II*, Can. J. Math. *23* (1971), 816–832.
8. J. M. Goethals and J. J. Seidel, *Orthogonal matrices with zero diagonal*, Can. J. Math. *19* (1967), 1001-1010.
9. R. C. Mullin, *A note on balanced weighing matrices*, Proc. Third Australian Conference on Combinatorial Mathematics, Brisbane, Australia, 1974.

10. R. C. Mullin and R. G. Stanton, *Group matrices and balanced weighing designs*, Utilitas Mathematica *8* (1975), 277–301.

11. R. E. A. Paley, *On orthogonal matrices*, J. Math. and Physics *12* (1933), 311–320.

12. V. Pless, *Symmetry codes over GF*(3) *and new five designs*, J. Comb. Theory *12* (1972), 119–142.

13. C. R. Rao, *Cyclical generation of linear subspaces of finite geometries*, Proc. Conf. on Combinatorial Mathematics and its Applications, 1967, University of North Carolina, Chapel Hill (1969), 515–535.

14. J. Singer, *A theorem on finite projective geometry and some applications to number theory*, Trans. Amer. Math. Soc. *43* (1938), 377–385.

15. S. S. Shrikhande, *Generalized Hadamard matrices and orthogonal arrays of strength two*, Can. J. Math. *16* (1964), 736–740.

16. G. A. Vanstone and R. C. Mullin, *A note on the existence of weighing matrices* $W(2^{2n-j}, 2^n)$ *and associated combinatorial designs*, Utilitas Mathematica *8* (1975), 371–381.

17. F. Yates, *Complex experiments*, J. Roy. Soc. Stat. *B2* (1935), 181–223.

University of Waterloo,
Waterloo, Ontario

https://doi.org/10.4153/CJM-1978-086-8 Published online by Cambridge University Press